UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,018	01/03/2001	Motoshi Ito	YAMAP0748US	3434

7590 11/23/2007

Neil A. DuChez
Renner, Otto, Boisselle, & Sklar, L.L.P.
19th Floor
1621 Euclid Avenue
Cleveland, OH 44115

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
11/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

7

Office Action Summary	**Application No.** 09/754,018	**Applicant(s)** ITO ET AL.	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3 and 6-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3 and 6-9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

This action is in response to the communication filed on 9/21/2007.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 9/21/2007 have been fully considered and are not found persuasive for the reasons presented below.

The examiner notes that the newly added limitations pertaining to the content of the recovered program is merely non-functional descriptive language, and as such does not further limit the scope of the claims, but rather provides insight into what a program could contain. The addition of the words "by the microprocessor", only provides that some data is to be called by the microprocessor, but does not actually require the functionality of calling the recovered program by the microprocessor. There is no language that functionally links the newly added language to the system, method, or computer readable medium, and as such is merely data. However, the examiner has cited Anderson et al. as showing that programs of the nature claimed were obvious to the ordinary person skilled in the art at the time of invention.

Regarding applicants' argument that Anderson does not specifically teach that a recovered program from an encrypted program includes a public function, an internal function, and a relative address list, the examiner does not find the argument persuasive. Anderson is relied upon as teaching, as was known and common in the art, that programs, in general, can include a public function, an internal function, and a relative address list. Hirotani on the other hand teaches that an encrypted program can be recovered to a non-encrypted program. Hirotani provides no limitations of the nature of the encrypted program, and as such one of ordinary skill in the art would find it obvious that the recovered program (i.e. the program before encryption and after decryption) could include a program according to the commonly known object oriented programming style, as claimed, and as taught by Anderson. Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument that altering Hirotani according to the teachings of Schneier would destroy the principle of operation of Hirotani, the examiner does not find the argument persuasive. First, although Hirotani disclosed that the decryption is performed by software, and does not disclose performing the decryption via hardware, this is merely the preferred embodiment of Hirotani. Nowhere in Hirotani is it taught that the decryption should not or cannot be performed using hardware. The purpose of Hirotani is to decrypt encrypted software without risk of the decryption algorithm being extracted from the device. One of ordinary skill in the art at the time of invention would have recognized, based upon the teachings of Schneier, that hardware decryption would not compromise this purpose, as Schneier on Page 224 teaches that encryption hardware can be securely encapsulated thereby eliminating the risk of access to the algorithm. Schneier further teaches advantages to using dedicated hardware module as opposed to a microprocessor and software, as taught by Hirotani, because software encryption is expensive to maintain. As such, based upon the teachings of Schneier, one of ordinary skill in the art would have found it obvious to modify Hirotani in the manner suggested by the examiner. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that one of ordinary skill in the art would be unable to determine how to modify Hirotani to implement a hardware solution that performs all the features of the software solution, the examiner does not find the argument persuasive. Schneier teachings are with regards to cryptography. As such, it would be obvious and clear to the ordinary person skilled in the art that in the combination, the decryption means of Hirotani would be replaced with a hardware decryption chip, as taught by Schneier. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that Schneier specifically states that it "is cheaper to put special-purpose encryption hardware in [devices] than it is to put in a microprocessor...", the examiner does not find the argument persuasive. The examiner points out that if the applicants were to continue reading this line of Schneier, the applicants would find that the full teaching of Schneier is that it "is cheaper to put special-purpose encryption hardware in [devices] than it is to put in **a microprocessor and software**". What this sentence means is that it would cost more to place a microprocessor and software into a device for encryption processing (this is what Hirotani disclosed), and it would cost less to use special purpose encryption hardware. In other words, Schneier is stating that an advantage of special purpose encryption hardware is that it costs less than microprocessors programmed with encryption software. As such, on of ordinary skill in the art would see this advantage and find it obvious to modify Hirotani to use special purpose encryption hardware as opposed to software. As such the examiner does not find the argument persuasive.

Regarding applicants' argument that Oishi in view of Elabd does not teach a data scramble circuit that is a single hardware circuit, the examiner does not find the argument persuasive. Neither the claim language, nor the specification, define "circuit" as anything more or less specific than how it is commonly used in the art. That is, a circuit is a combination of electrical components interconnected to perform a particular task. At one level, a computer is a single circuit; at another, it consists of hundreds of interconnected circuits. This is because a circuits boundaries are relative to the perspective. As such, a system on a chip is "a circuit", and as discussed below, it would be obvious to the ordinary person skilled in the art to implement the system of Hirotani, Schneier, and Oishi in a system on a chip. As such, the combination meets this limitation of the claim language, and the examiner does not find the argument persuasive.

Regarding applicants' argument that Murakami does not teach a data scramble circuit that performs error correction, the examiner does not find the argument persuasive. Replacing missing bits of data is error correction, which the decoding circuit of Murakami performs. As such, the teachings of Murakami render obvious this claim limitation. Therefore, the examiner does not find the argument persuasive.

Because the examiner does not find the arguments persuasive, the previous prior art rejections have been maintained.

All objections and rejections not presented below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirotani (US Patent Number 5,982,887), further in view of Oishi (US Patent Number 6,907,125), and further in view of Schneier (Applied Cryptography), and further in view of Elabd (US Patent

Number 6,526,462), and further in view of Anderson et al. ("Navigating C++ and Object-Oriented Design"), hereinafter referred to as Anderson.

Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani also fails to disclose the use of a system on a chip design. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25 Program section); a rewritable memory for storing a copy of the concealed program copied from the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least temporarily in a rewritable memory in the decryption circuit, before decryption), and a data scramble circuit for recovering the concealed program stored in the rewritable memory as a recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 6, Hirotani disclosed a method for creating a control program, comprising: a program descramble step of descrambling a portion of a control program by reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a concealed program as a portion of the control program (it was inherent in the invention of Hirotani that a portion of the control program was encrypted in order for the control program to have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control program including the concealed program in a program memory so that the control program controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines

39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 8, Hirotani disclosed a method for operating a control program, comprising: a program copying step of copying a concealed program which is a portion of the control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable memory (See rejection of claim 3 above); a program recovery step of recovering the concealed program copied by the program copying step as a recovered program by a data scramble circuit (See rejection of claim 3 above); and a program execution step of executing a non-concealed program included in the control program and the recovered program (See Hirotani Col. 6 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 7, the combination of Hirotani, Oishi, Schneier, Elabd, and Anderson disclosed that the program descramble step includes the steps of: creating a non-concealed program (it was inherent that the program was created at some point in order for the program to have been encrypted and downloaded); and synthesizing the concealed program and the non-concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the encrypted and non-encrypted programs are together as the program stored in program memory).

Regarding claim 9, the combination of Hirotani, Oishi, Schneier, Elabd, and Anderson disclosed a program erasure step of erasing the recovered program from the rewritable memory (See Hirotani Col. 6 Paragraph 6).

Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirotani (US Patent Number 5,982,887), further in view of Murakami et al. (US Patent Number 5,613,005) hereinafter referred to as Murakami, and further in view of Schneier (Applied Cryptography), and further in view of Elabd (US Patent Number 6,526,462), and further in view of Anderson et al. ("Navigating C++ and Object-Oriented Design"), hereinafter referred to as Anderson..

Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani also fails to disclose the use of a system on a chip design. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25 Program section); a rewritable memory for storing a copy of the concealed program copied from the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least temporarily in a rewritable memory in the decryption circuit, before decryption), and a data scramble circuit for recovering the concealed program stored in the rewritable memory as a recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 6, Hirotani disclosed a method for creating a control program, comprising: a program descramble step of descrambling a portion of a control program by reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a concealed program as a portion of the control program (it was inherent in the invention of Hirotani that a portion of the control program was encrypted in order for the control program to have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control program including the concealed program in a program memory so that the control program controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines 39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 8, Hirotani disclosed a method for operating a control program, comprising: a program copying step of copying a concealed program which is a portion of the control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable memory (See rejection of claim 3 above); a program recovery step of recovering the concealed program copied by the program copying step as a recovered program by a data scramble circuit (See rejection of claim 3 above); and a program execution step of executing a non-concealed program included in the control program and the recovered program (See Hirotani Col. 6 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program by the microprocessor and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176); and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of

Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product. Further still, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Anderson in the recovered program of Hirotani by having both a public and private portion and having the public portion called from outside the program and having the private portion called from inside the public portion, and having a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow simple lookup schemes to call functions from a table entry, as well as to provide encapsulation to the program.

Regarding claim 7, the combination of Hirotani, Murakami, Schneier, Elabd, and Anderson disclosed that the program descramble step includes the steps of: creating a non-concealed program (it was inherent that the program was created at some point in order for the program to have been encrypted and downloaded); and synthesizing the concealed program and the non-concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the encrypted and non-encrypted programs are together as the program stored in program memory).

Regarding claim 9, the combination of Hirotani, Murakami, Schneier, Elabd, and Anderson disclosed a program erasure step of erasing the recovered program from the rewritable memory (See Hirotani Col. 6 Paragraph 6).

Conclusion

Claims 1, 3, and 6-9 have been rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew Henning/
Assistant Examiner
Art Unit 2131
11/19/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100